Optimized and Secured Transmission and Retrieval of Vital Signs from Remote Devices

Shanti R. Thiyagaraja, Ram Dantu, Pradhumna L. Shrestha, Mark A. Thompson, Christopher Smith
Department of Computer Science and Engineering, University of North Texas, 3940 N. Elm St.,
Denton, TX 76207-7102
shantimdhv@gmail.com, {ram.dantu, mark.thompson2, pradhumna.shrestha} @unt.edu,
christophersmith14@my.unt.edu

***Abstract*— Smartphones and other mobile platforms provide a low cost and easily accessible method of monitoring patient health, and aid healthcare professionals in early detection of disease. Immediate access to the gathered data is an essential factor in effective patient care. But the current processes used for patients' vital data collection is slow and error prone. This undermines the advantages of remote monitoring that mobile platforms for health monitoring provide. In this paper, we propose to upload the patient health information to the Cloud. We investigate three different models to transfer data from the smartphone to the Cloud—perform all computations in the smartphone, perform all computations in the Cloud, and divide the computations between the smartphone and the Cloud. The second approach was found to be infeasible due to very high latency in data transfer with a delay of 2.84 seconds at an upload speed of 2500 KBytes per second.**

In order to protect the privacy of patients, it is required by law that the data gathered from remote monitoring by using mobile platforms must be kept private, and be secured before uploading to the Cloud. This paper explores the use of prominent public key encryption algorithms and their performance on a mobile device to securely transmit confidential electronic personal health information to the Cloud. We analyze performance of three common public key encryption schemes –RSA, Diffie-Hellman, and ECC. It is shown that 160 bit key size in ECC scheme provides the same level of security that a 1024 bit key size does in RSA and Diffie-Hellman. Further, the encryption and decryption time required by ECC is three times less than the other two schemes. Hence, ECC not only requires a smaller key size to provide the same level of security, but also faster encryption and decryption times as compared to the other two schemes. This makes ECC algorithms suitable to be implemented in resource constrained mobile platforms. We also compared ECC curves from three different standards – NIST, SECG, and Brainpool – to determine the optimum ECC curve, and key size to encrypt data in the mobile phone platform. It is shown that the Brainpool curve performed better than the other two standards when the key size is less than 521 bits. We also measured the latency of uploading encrypted data in a wide variety of WiFi and mobile networks.

Keywords—Cloud Computing, Mobile Health, Security, Performance Evaluation

I. INTRODUCTION

According to a survey published by The US Department of Health and Human Services in 2014, 27.6 million adults report that a doctor or other healthcare professional diagnosed them with heart disease [1]. According to the National Vital Statistics Reports [2], heart disease is the leading cause of death among adults in the US. Early detection of heart disease is essential for doctors to prescribe life-saving treatments to patients. However, many individuals do not recognize that they suffer from heart disease until their health is in danger. A national ambulatory medical care survey [3] detailed that patients with heart disease make 12 million visits to physicians' offices annually, which is less than half the number of diagnosed cases reported above. Accessible forms of continuous healthcare monitoring can help people maintain awareness about their health rather than waiting until an emergency or annual physician's exam.

Currently, disease symptoms such as abnormal cardiac cycles require professional training to identify and diagnose because of the sophisticated interpretation requirements of the acoustic signals. However, healthcare software applications [4, 5] can turn mobile platforms such as smartphones into low cost measurement devices for home health care. A person will be able to use smartphone accessories to measure vital signs such as blood pressure and heart and lung sounds. Mobile healthcare applications can then process the person's health information and alert them to signs of possible disease. Along with providing a remotely manageable and portable solution, smartphones also allow quick and reliable access of the collected health data via mobile network.

Access to medical records is another important factor in patient care. Electronic Medical Records (EMR) give physicians, labs, and other health care providers access to patient information from many different facilities. Unfortunately, at this time, access is generally limited to one health care facility such as a specific hospital or doctor's office.

Existing processes for patients' vital data require a great deal of labor to collect, input and analyze the information. These processes are usually slow and error prone, introducing a latency that prevents real-time data accessibility. This scenario restrains the clinical diagnostics and monitoring capabilities. The authors in [6] propose a solution to automate this process from bedside data collection to information distribution and remote access by medical staff.

978-1-5090-4722-2/17 $31.00 © 2017 IEEE
DOI 10.1109/CHASE.2017.55

A cloud storage and computing platform that provides real-time upload and retrieval of patients' health information complements the remote monitoring capabilities of the mobile health platforms very well, and together provide an effective system for patient care. In this paper, we analyze three different models of uploading data to the Cloud and compare their performances in order to find the optimum distribution of data analysis and processing between the smartphone platform and the Cloud.

According to the "Security Standards for the Protection of Electronic Protected Health Information" rule found in Title 45 of the US Code of Federal Regulations, Parts 160 and 164 in Subsections A and C [7], any PHI shared with a bounded entity or business, such as a physician, must be encrypted. Therefore, the data collected by the smartphone must be secured before uploading it to the Cloud. Implementing a data security mechanism on mobile phone platforms require special consideration of the limited computing resources available. Different cryptographic systems, while providing the same level of security, may incur different costs on processing, transmission, and storage resources across different platforms. In this paper, we analyze the performance of different public key cryptographic algorithms on preprocessed heart sound data files across multiple networks.

The rest of the paper is structured as follows. In Section II, we discuss our objectives of the paper. In Section III, we discuss efficient uploading and retrieval of patient health information to and from the Cloud. In Section IV, we present our analysis on securing the patients' health information on a smartphone platform. Finally, we conclude our paper in Section V.

II. Objectives

A. Optimal Transmisson and Retrieval of Patient Health Information

In [5], we presented a novel method of measuring heart rate and blood pressure using smartphones. We collected the audio data from the heart sounds using a customized external microphone and the video signals of the finger pulses using the smartphone camera. This remotely monitored and collected data must be readily accessible by a healthcare professional to appropriately care for the patient. However, current technologies employed in accessing medical records of patients has high latency and is error prone. Therefore, our primary objective is to make the collected audio and video signals accessible.

While instant and reliable access of health data is critical in efficient patient care, we must also consider the requirements of the costs incurred on the mobile platform in making the data available. The audio and video signals collected for vital signs comprise a large amount of data, and the processing and transmitting of this data has high costs. Therefore, we have to design an efficient transmission and retrieval process so that connections remain stable and reliable. Furthermore, we also have to consider the processing abilities of the remote devices such as smartphones used in the remote monitoring.

In section III, we present a wireless data transmission scheme, which can be used to upload data to the Cloud. Also, depending on the processing capabilities of the smartphone device and the cloud server, there are different scenarios for uploading data to the Cloud:

i) Perform all data analysis and computations on the remote device collecting the data
ii) Perform all data analysis and computations in the Cloud
iii) Partially compute and analyze data on the remote device and upload to the Cloud and then complete the remaining analysis and computations in the Cloud

We analyze these three different models of data processing in order to investigate the best strategy to process and upload the multimedia data related to patients' health.

B. Optimal Performance in Securing Data in Smartphone

Securing patients' health information is critical as well as legally required before we can upload the data to the Cloud. There are multiple encryption schemes available for securing data before transmission. However, due to limited resources available on a mobile platform, it may not be feasible to run a particular encryption mechanism because of the associated costs of storage, power, and processing time. We need to take into account that the processing and uploading of large amounts of audio and video signal to the Cloud is already incurring huge computational and storage costs on the remote devices, and the requirement to encrypt will increase these costs even further. We consider the following aspects of the encryption mechanism, which are discussed in detail in Section IV.

1) Selecting a suitable encryption mechanism

Due to limited resources on a mobile platform, a lightweight public key encryption mechanism is preferred. Various public key cryptographic methods have different computing requirements such as key size, and encryption and decryption times, even for the same level of computing security. Due to limited power and processing capabilities of a smartphone platform, selecting an appropriate securing mechanism that best fits the requirements of the platform is critical.

2) Performance evaluation of encrypton mechanism

Even after selecting a suitable algorithm to implement on the smartphone platform, it is necessary to investigate the actual performance of the data security mechanism. From the security point of view, higher levels of encryption, i.e., larger key size, may be better. But it will come at the cost of performance. A decent trade-off between the level of security and the performance of the system is necessary and needs to be investigated. Also, it is necessary to test the latency associated with the upload of the encrypted data in diverse network environments.

III. Storage and Retrieval From The Cloud

To provide efficient care, continuous and remote monitoring of patients' health information is necessary. Health application software in a smartphone platform provide a remarkable mechanism to implement such a monitoring system with added benefits of being cost effective, portable, and easily accessible. Along with the capability of data collection and monitoring, instant access of data is also critical for effective care. The mechanisms for transmitting the collected data from a smartphone to a server, and retrieving the data from the same

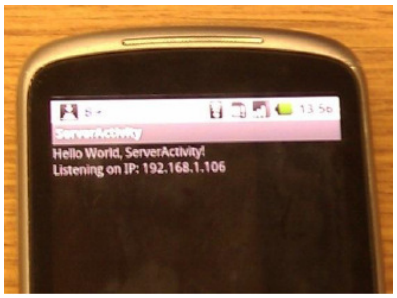

Figure 1(a): Screenshot of the server listening for the client

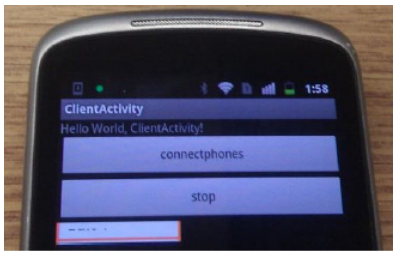

Figure 1(b): Screenshot from the client

server by physicians and health care providers are necessary. Furthermore, such mechanisms should have very low latency for quick access and very high accuracy. We have proposed to use a cloud-based solution for reliable and immediate access of data collected by the smartphone-based health applications. In this section, we will demonstrate how data can be reliably transmitted and retrieved from a smartphone.

In [8], the authors have presented a novel eHealth services platform designed by the Data Capture and Auto Identification Reference (DACAR) project [9]. Its aim is to develop and implement an "in-the-Cloud" service platform for capture, storage and consumption of medical data. In [10], the authors have presented an implementation of a mobile system that enables electronic healthcare data storage, update, and retrieval using Cloud Computing.

More specifically, we will demonstrate the capability of transmission and retrieval of data from a smartphone to a server using a WiFi connection. However, the same principles can be applied to upload the collected the data to a dedicated or commercial cloud server using the mobile data network already available with the smartphone.

A. *Data Transmission from a Smartphone*

The first step in uploading the data to the Cloud is transmitting the data from a smartphone that is collecting the information. Figures 1(a) and 1(b) shows the data transmission between two smartphones, where one smartphone is acting as the remote user and the second smartphone is acting as the server. In this demonstration, we are transmitting heartbeat data between smart phones, but the concept is not limited to a particular type of health metric. The same system can also transmit other vital signs such as blood pressure and lung sounds in the same manner.

A performance evaluation of the accuracy of data transmission application is shown in Table 1. Table 1 shows the number of heart beats sent from the client and received at the server. It can be observed that there is no loss in accuracy of heart beat data at the receiver's end.

TABLE 1: HEART BEATS TRANSMITTED FROM THE CLIENT AND RECEIVED AT THE SERVER SHOWING NO LOSS OF DATA

Heartbeats Sent	Heartbeats Received
70	70
77	77
78	78
66	66
74	74
69	69

B. *Distrubution of Processing between Smartphone and the Cloud*

The audio and video signals [5] collected by the remote smartphones need to processed as well as uploaded. Due to the volume of data collected, data processing as well as uploading incurs large costs on the computing and storage resources. This cost requirement gets magnified on resource-constrained mobile platforms such as smartphones. The Cloud computing platform, on the other hand, may have a relatively higher computing power as well as storage capabilities. Therefore, an investigation of optimal distribution of processing of the collected audio and video data between the smartphone and the Cloud is essential for an efficient system. Here, we will analyze three models for uploading data from the smartphone health application to a server, and investigate which model works best for a smartphone platform. In this experiment, we will be uploading both audio and video files from the smartphone application [5] to a server, which is a computer acting as the Cloud. Three scenarios for distributing the data processing responsibilities have been analyzed.

1) Model 1: Data Analysis and Computation Fully Done on the Smartphone

In this model, once the remote user collects the data using the smartphone application, the video and audio signals are processed and analyzed in the smartphone. Later, the final calculated values of the blood pressure and the heart rate are

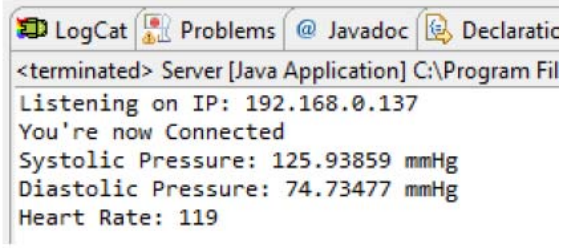

Figure 2: Screenshot showing the uploaded blood pressure and heart rate values on the server

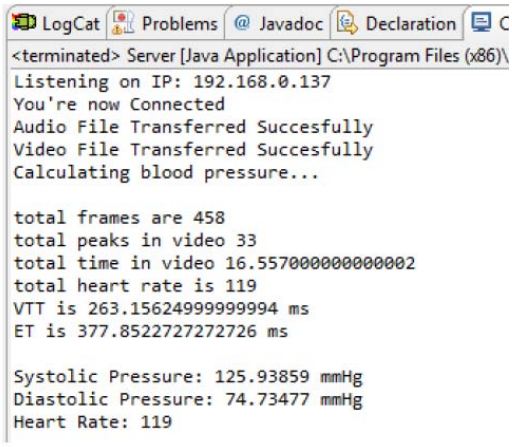

Figure 3: Screenshot showing the audio and the video data being uploaded, and blood pressure and heart rate value being calculated on the

uploaded to the server. Figure 2 shows the display of blood pressure and the heart rate values in the server.

2) Model 2: Data Analysis and Computation Fully Done on the Server

In this model, instead of processing the video and audio signal in the smartphone, the recorded audio and video signals are uploaded to the server immediately after the measurement is taken. The server receives the data, subsequently processes and analyzes it, and finally computes the blood pressure. The screenshot in Figure 3 from the server shows the files being transferred to and processed in the server, and the final blood pressure and heart rate values being computed.

3) Model 3: Data Analysis and Computation Partially Done on both the Smartphone and the Server

In this model, the audio and video signals are processed in the smartphone first. The processed data in the smartphone contains the peak values of the audio and video signals. Next, the processed data is uploaded to the server for further computation of the blood pressure and the heart rate. Once the data is uploaded, the server computes the blood pressure and the heart rate based on the peak values. Figure 4 shows the computed blood pressure in the server. When compared with Figure 3, the computations of peak values are missing, which is actually done in the smartphone in this case.

To evaluate the performance of the three uploading models, we calculated the latency, which is time taken to upload the files using the three models. In Table 2, we show the time taken to upload the data from the smartphone to the server, the data size, and the average bytes per second for the three models. We perform the experiment in two different types of WiFi networks. The lab network represents typical broadband WiFi connections available in hospital settings, while the home network represents a remote clinic or a health care professional working from home.

As seen in Table 2, using Model 2 for uploading data to the Cloud is not feasible. The unprocessed audio and video data size is large, and uploading the data has high latency, especially on a

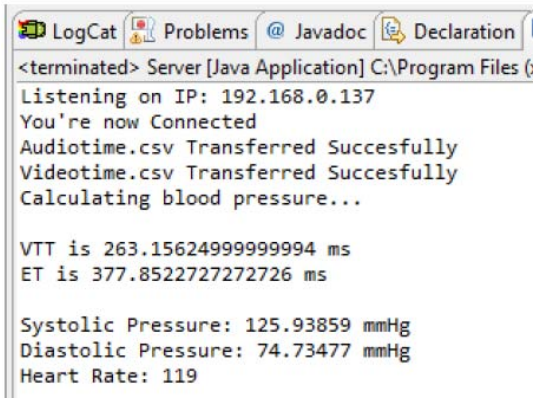

Figure 4: Screenshot showing transfer of audio and video files on the server and computation of blood pressure on the server

home network. Model 1 has much lower latency as we are only uploading the final blood pressure and heart rate measurements, but all the processing load is on the smartphone application. Model 3 has a slightly higher latency, but the smartphone application has limited processing responsibility. The selection between Models 1 and 3 largely depends on the smartphone processing capabilities and resources, and the application running on it.

C. Retrieval of data from the server

TABLE 2: LATENCY MEASUREMENT OF THE THREE MODELS EVALUATED IN LAB AND HOME NETWORK CONDITIONS

Networks	Lab Network			Home Network		
Models	1	2	3	1	2	3
Data Size (Bytes)	750	7107114	1652	750	7107114	1652
Duration (sec)	0.13	2.84	0.18	0.15	27.37	1.02
Avg. Kbytes/sec	5.8	2500.9	9.0	5.1	259.6	1.6

A physician or a healthcare professional must be able to access of the data from the Cloud with minimal latency and high accuracy. In this section, we upload a processed audio file with heartbeat signal from the smartphone to the server, and then download the data from the server to another smartphone. The latter smartphone represents the medical practitioner's smartphone. The latency time is measured and tabulated in Table 3.

TABLE 3: RETRIEVAL TIME TO DOWNLOAD DATA FROM THE SERVER

Networks	Lab Network	Home Network
Data size (bytes)	478	478
Duration (sec)	0.123	0.16
Avg. KBytes/sec	3.9	2.7

It must be noted that the vital signs discussed in this section are examples of the data that can be transmitted to the server. The actual application itself is not limited only to the vital signs mentioned in this section. Furthermore, using a second

smartphone as a server and connecting to the server via WiFi is only representational. Smartphones are already part of the mobile data network, and can use the mobile data connection instead of WiFi to upload data to the server. Also, the smartphone being used as the server is simply representing the Cloud. A dedicated or a commercial Cloud platform is easily accessible to the client smartphone via the mobile data network, and the same transmission strategies discussed in this section will work with such cloud platforms as well.

IV. Securing Electronic Medical Data

Before uploading any patient health information on the Cloud, it is legally required that the data be encrypted. In this section, we will analyze various prominent encryption schemes available and evaluate their performance.

A. Selection of an Encryption Mechanism

Smartphones have limited resources to run encryption algorithms. Hence, lightweight cryptographic techniques to secure data are used.

In [11], the authors compared three notable public key systems – RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC). A summary of the results from [11] is presented in [12]. In [11, 12], it is seen that ECC can provide the same level of security, as represented by the number of security bits, using a smaller key size compared to the other two algorithms. For example, for 80 security bits, RSA and Diffie-Hellman requires a key size of 1024 bits, whereas ECC only requires key size of 160-223 bits.

Both the ECC and the RSA encryptions were implemented in the same smartphone, and their performance for the same level of security was compared [12]. The encryption and the decryption times were used to measure the performance and are tabulated in Table 4. From the 160-bit ECC vs 1024-bit RSA comparison, we can see that the elliptic curve algorithm is approximately three times faster than the RSA algorithm. Hence, the ECC not only requires a smaller key size, but is also faster. Therefore, it has lower storage as well as computational requirements. This performance gain is very significant for the smartphone platforms with limited computing power and storage resources. Therefore, ECC is the recommended scheme for encryption of patient health information before uploading to the Cloud.

TABLE 4: COMPARISON OF ENCRYPTION AND DECRYPTION TIMES IN MILLISECONDS OF ECC AND RSA FOR THE SAME LEVEL OF SECURITY

Elliptic Curve Key Size	160-bit	224-bit	256-bit	384-bit
Encryption Time (ms)	189	477	1044	2188
Decryption Time (ms)	190	450	1080	1786
RSA Key Size	1024-bit	2048-bit	3072-bit	7680-bit
Encryption Time (ms)	576	1921	4124	7890
Decryption Time (ms)	580	1893	4246	7722

Each standards organization maintains different elliptic curve identifiers. A performance analysis was also done on elliptic curves from different identifiers such as NIST [13], Standards for Efficient Cryptography Group (SECG) [14] and ECC Brainpool [15] in order to determine the best ECC curve for the smartphone platform. The encryption time for each type of ECC curve for different key sizes is tabulated in Table 5. The Brainpool curves seem to perform better compared to other curves when the key size is smaller than 521 bits.

TABLE 5: COMPARISON OF ENCRYPTION TIME (IN MS) OF THREE ECC IDENTIFIER CURVES FOR DIFFERENT KEY SIZES

Key Size	SECG Curves (ms)	Brainpool Curves (ms)	NIST Curves (ms)
192	867	832	933
224	1180	907	1190
256	1105	1088	1339
384	2315	2188	2283
521	2760	3428	3266

B. Performance Analysis of Encryption Mechanism

To analyze the performance of the Brainpool curve implementation on a multimedia medical record containing an audio file, we encrypted three different audio files of different file size. We selected the key size to be 256 bits. The time required to encrypt and decrypt each file is shown in Table 6. This time represents the actual latency created by the need to secure data before transmission. This is important not only from the point of view of computational efficiency of the mobile and the Cloud platforms, but also from the point of view of delay in accessing the remotely collected data.

TABLE 6: ENCRYPTION AND DECRYPTION TIMES OF THREE AUDIO FILES USING ECC BRAINPOOL CURVE OF 256 BITS KEY SIZE

Audio File	1	2	3
File Size (KB)	184	231	401
Encryption time (ms)	3489	3600	7279
Decryption time (ms)	3322	3457	7123

To evaluate the performance of uploading encrypted data, the encryption algorithm was built on the smartphone to encrypt three files having a total size of 5 MB, with each file containing one of the following types of data:

- '.csv', comma separated values, of a heart sound plot
- Image of the diagnosis and the heart sound waveform
- Audio recording of the heart sound

The server, which is a computer, receives the three files and decrypts them. The files were uploaded to the server from the smartphone in a wide variety of networks to analyze the upload

time or latency. The upload speeds and the corresponding upload time at different locations are presented in Table 7.

TABLE 7: COMPARISON OF UPLOAD TIMES OF ENCRYPTED DATA IN DIFFERENT NETWORKS

Place	Elapsed time (s)	Upload speed (MB/s)
University of North Texas Campus – Discovery Park(Wi-Fi)	1.968	3
Home (Wi-Fi)	2.191	2
DFW Airport (4G)	21.714	0.3
UNT Main Campus (4G)	6.359	0.9
Rural Area (4G)	15.289	0.4

V. CONCLUSION AND FUTURE WORK

Smartphone applications provide a remote, cost-effective, portable, and easy-to-use health-related data collection mechanism for patients. For effective care, however, along with remote monitoring of patients, quick access of collected vital signs by health care professionals is essential. In this paper, we demonstrated the viability of using the cloud computing and storage platform for this purpose. The smartphones are already a part of a mobile network and have easy access to the Cloud. We demonstrated using suitable experiments that the health-related data can be accurately uploaded to the Cloud and then retrieved from the Cloud by a medical practitioner.

While uploading patients' health information to the Cloud, we must consider how to optimally divide the data analysis and processing responsibilities between the smartphone and the Cloud. In this paper, we presented three models:

- Data is completely analyzed and processed in the smartphone
- Data is completely analyzed and processed in the Cloud
- Data is partially analyzed and processed in the smartphone, uploaded to the Cloud and the remaining processing and analysis is performed in the Cloud

We computed the latency associated with the upload of the data, and showed that the second model was not feasible due to the high latency it will cause in data delivery. Therefore, we concluded that the first or the third model should be adopted for uploading the medical data to the Cloud.

Before uploading patients' health information to the Cloud, it is legally required that the data is encrypted before the upload. In this paper, we also investigated the optimal approach to perform such encryption. Due to limited computing resources available in the smartphone platform, a lightweight public key encryption scheme was preferred. We compared three different common encryption schemes—RSA, Diffie-Hellman, and ECC. We found that the ECC requires a smaller key size than the other two schemes to provide the same level of security. We also showed via experimentation that the smaller key size requirement directly leads to a faster encryption and decryption time. This performance gain is significant for a smartphone platform with limited resources. Hence, we concluded that the ECC scheme is the most suitable method of encrypting data in the smartphone. We also compared the performance of three common elliptic curve identifiers maintained by three different standards—NIST, SECG and Brainpool. We demonstrated that for key size of less than 521 bits, the Brainpool curve results in a faster encryption time. We also computed the latency of the upload of the encrypted data in both mobile and WiFi networks.

For future work, our current efforts are in developing a real-time remote access and control mechanism supported by the presented smartphone and Cloud platform. The real-time access and control would require more sophisticated and optimized processing in the smartphone platform. The research challenge will be to aptly use the limited resources available in the smartphone to support real-time applications.

REFERENCES

[1] Summary Health Statistics Tables for U.S. adults: National Health Interview Survey, 2014, ftp://ftp.cdc.gov/pub/Health_Statistics/NCHS/NHIS/SHS/2014_SHS_Table_A-1.pdf

[2] Deaths: Final Data for 2013, 2013, http://www.cdc.gov/nchs/data/nvsr/nvsr64/nvsr64_02.pdf

[3] National Ambulatory Care Survey: 2012 State and National Summary Tables,2012, http://www.cdc.gov/nchs/data/ahcd/namcs_summary/2012_namcs_web_tables.pdf

[4] S. R. Thiyagaraja, J. Vempati, R. Dantu, T. Sarma, and S. Dantu, "Smart phone monitoring of second heart sound split, 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, IEEE, 2014, pp. 2181-2184.

[5] V. Chandrasekaran, R. Dantu, S. Jonnada, S. Thiyagaraja, and K. P. Subbu, "Cuffless differential blood pressure estimation using smart phones", IEEE Transactions on Biomedical Engineering, Vol. 60 Issue , no. 4, April 2013, pp. 1080-1089.

[6] C. O. Rolim, F. L. Koch, C. B. Westphall, J. Werner, A. Fracalossi, G.S. Salvador, "A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions," Second International Conference on eHealth, Telemedicine, and Social Medicine, 2010. ETELEMED '10, pp.95-99.

[7] Electronic Code of Federal Regulations, 2016, http://www.ecfr.gov/cgi-bin/text-idx?SID=ffd51b7ba25febde9b337624bb31617e&mc=true&node=se45.1.160_1103&rgn=div8

[8] L. Fan, W. Buchanan, C. Thummler, O. Lo, A. Khedim, O. Uthmani, A. Lawson, D. Bell, "DACAR Platform for eHealth Services Cloud," 2011 IEEE International Conference on Cloud Computing (CLOUD), pp.219-226, 4-9 July 2011

[9] "Data Capture and Auto Identification Reference Project", TSB/EPSRC project number 400092, www.dacar.org.uk.

[10] C. Doukas, T. Pliakas, I. Maglogiannis, "Mobile healthcare information management utilizing Cloud Computing and Android OS," 2010 Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp.1037-1040, Aug. 31 2010-Sept. 4 2010

[11] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "NIST special publication 800-57", NIST Special publication 800 (2007), no. 57, 1-142.

[12] S. R Thiyagaraja, "Detection and Classification of Heart Sounds using a heart-mobile interface", A Dissertation, Univ. of North Texas, 2016

[13] Recommended elliptic curves for federal government use, 1999, http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf.

[14] Standards for efficient cryptography (SEC 1), Ver 2, 2009, http://www.secg.org/download/aid-780/sec1-v2.pdf.

[15] ECC Brainpool standard curves and curve generation, 2005, http://www.ecc-brainpool.org/download/Domain-parameters.pdf.